IN THE CLAIMS:

No claim amendments are being made herein. The claims are being reproduced merely for the Examiner's convenience.

1. (Previously Presented) A method for managing access to a scrambled event of a service provider, said method comprising:

receiving in a device an electronic list of events available from one or more sources, each event having a digital signature and an encrypted message associated therewith;

receiving in the device, in response to user selection of one of the events from the list of events, the digital signature and the encrypted message associated with the selected event, the digital signature being encrypted with a first key and the encrypted message being encrypted with a second key different from the first key, the encrypted message comprising a descrambling key and event information including at least one of a channel identity, date and time stamp, event identity and payment amount corresponding to the selected event;

authenticating in the device a source of the digital signature and the encrypted message associated with the selected event by decrypting the digital signature in response to receiving the digital signature and the encrypted message;

decrypting in the device the encrypted message to obtain the descrambling key upon the authenticating;

receiving in the device the selected event from the service provider, the selected event being scrambled using the descrambling key for preventing unauthorized access to the selected event; and

descrambling in the device the selected event using the descrambling key.

2. (Previously Presented) The method of Claim 1 wherein the device comprises a smart card and the steps of decrypting the message, receiving the selected event, and descrambling the selected event are performed in the smart card, and

wherein the second key is a first public key associated with the smart card and the step of decrypting uses a first private key associated with and stored in the smart card.

3.	(Previously Presented) The method of Claim 2 wherein the message further comprises event information, the event information being decrypted using the private key.

4.	(Previously Presented) The method of Claim 3 further comprising the step of storing the event information, wherein the step of storing the event information is performed in the smart card.

5.	(Previously Presented) The method of Claim 4 wherein the smart card has a card body having a plurality of terminals arranged on a surface of the card body in accordance with one of ISO 7816 and PCMCIA card standards.

6.	(Previously Presented) The method of Claim 5 further comprising authenticating the list of events to verify the origin of the message.

7.	(Previously Presented) The method of Claim 6 wherein the first key is a second private key and the step of authenticating comprises decrypting the digital signature using a second public key that is stored in the device.

8.	(Previously Presented) The method of Claim 4 wherein the event information comprises channel identification data, event identity data, date and time stamp data, and billing data.

9.	(Previously Presented) The method of Claim 3 further comprising the step of storing the event information, wherein the step of storing the event information is performed in the device.

10.	(Previously Presented) The method of Claim 7 wherein the digital signature, the second public key and the second private key are issued by an independent certificate authority and are associated with the list provider.

11.	(Previously Presented) The method of Claim 10 wherein the device is a digital television.

12.	(Previously Presented) The method of Claim 10 wherein the device is a set-top box.

3

13. (Previously Presented) The method of Claim 4 wherein the event information is used within the device to update a user's account information.

14. (Previously Presented) The method of Claim 13 wherein the event information is downloaded to an independent billing center to update the a user's account information.

15. (Previously Presented) A method for managing access between a device having a smart card coupled thereto and a service provider, the device performing the steps of:

receiving an electronic program guide having a plurality of events from a guide provider, the guide having a message and a digital signature associated with each event in the guide, the message being encrypted using a public key of the smart card and the digital signature being created using a private key of the guide provider;

selecting an event from the guide;

receiving the encrypted message and the digital signature corresponding to the selected event;

authenticating the guide provider by decrypting the digital signature using a public key of the guide provider, the guide provider public key being stored in the device;

passing the message to the smart card;

decrypting, in the smart card, the message using a private key of the smart card to obtain event information and a symmetric key, the smart card private key being stored within the smart card;

storing the event information in the smart card and updating account information based on the event information;

receiving from the service provider the selected event, the selected event being scrambled using the symmetric key; and

descrambling, in the smart card, the selected event using the symmetric key to generate a descrambled event.

16. (Original) The method of Claim 15 wherein the device is a set-top box.

17.   (Original) The method of Claim 15 wherein the device is a digital television.

18.   (Previously Presented) A method for managing access between a device having a smart card coupled thereto and a service provider, the device performing the steps of:

receiving an electronic program guide having a plurality of events from a guide provider, the guide having a digital certificate and a separate message corresponding to each event in the guide, each of said digital certificates being encrypted using a first private key of the guide, the separate message being encrypted using a public key of the smart card and having an associated digital signature created using a second private key of the guide;

selecting an event from the guide;

receiving the digital certificate, the message and the digital signature corresponding to the selected event;

authenticating the guide provider by decrypting the digital certificate using a first public key of the guide to obtain a second public key of the guide, and decrypting the digital signature using the second guide public key, said first guide public key being stored in the device;

passing the message to the smart card;

decrypting, in the smart card, the message using a private key of the smart card to obtain event information and a symmetric key, the smart card private key being stored within the smart card;

storing the event information in the smart card and updating account information based on the event information;

receiving from the service provider the selected event, the selected event being scrambled using the symmetric key; and

descrambling, in the smart card, the selected event using the symmetric key to generate a descrambled event.

19.   (Original) The method of Claim 18 wherein the device is a set-top box.

20.   (Original) The method of Claim 18 wherein the device is a digital television.